CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6722.01A
DISTRIBUTION: A, B, C, J 1 July 2000

GLOBAL COMMAND AND CONTROL SYSTEM
CONFIGURATION MANAGEMENT POLICY

References: See Enclosure E.

1. Purpose. This instruction defines the configuration management (CM) policy for the Global Command and Control System (GCCS) and outlines organizational structure and processes that will improve the management and control of the GCCS. Implementation will result in reduced operational risk, better management information, more mature processes, fewer errors, and faster development.

2. Cancellation. CJCSI 6722.01, 1 July 1997, is canceled.

3. Applicability. This instruction applies to CINCs, Services, and agencies (C/S/A), the Joint Staff, and others who use GCCS. Its authority is derived from CJCS direction in reference a. NOTE: This instruction does not apply to Service-unique variations of the GCCS or to locally added items that do not interact with the GCCS.

4. Policy

a. For the purpose of this instruction, GCCS CM is the application of a disciplined process to ensure changes to GCCS and its documentation are identified, tracked, and implemented in a controlled, deliberate manner. The GCCS includes applicable portions of the following: automated data processing (ADP) hardware and software, communications hardware and software, and the Defense Information Systems Network (DISN).

b. New requirements shall be addressed in accordance with guidance outlined in reference b. For input to the CM process, only changes that satisfy validated functional requirements are acceptable. The GCCS

Configuration Management Board (CMB) will accept new functional requirements only from the Joint Staff, J3. The GCCS Problem and Change Review Board (PCRB) will accept designated problem reports (PR) and non-functional change requests (CR) as specified in its charter.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes

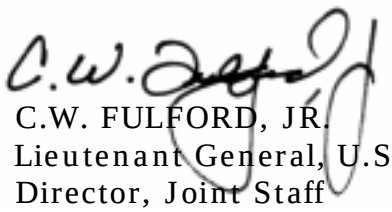
a. Reflects changes to CJSCI 6721, GCCS Management Structure.

b. Renames the GCCS Configuration Control Board to the GCCS Configuration Management Board (CMB).

c. Adds entry criteria and CMB exit criteria for C/S/A developed mission application consideration for addition to the GCCS baseline.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/doctrine. Copies are also available through the Government Printing Office or the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective upon receipt.



C.W. FULFORD, JR.
Lieutenant General, U.S. Marine Corps
Director, Joint Staff

Enclosures:
A - Responsibilities
B - GCCS CM Structure
C - GCCS CM Activities
D - GCCS CM Process
E - References
Glossary

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 2	O	C-1 thru C-4	O
i thru vi	O	D-1 thru D-10	O
A-1 thru A-10	O	E-1 thru E-2	O
B-1 thru B-8	O	GL-1 thru GL-16	O
B-A-1 thru B-A-2	O		

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

ENCLOSURE A

RESPONSIBILITES

1. Joint Staff. The Chairman of the Joint Chiefs of Staff is responsible for policy guidance and oversight of Global Command and Control (GCC). The Joint Staff, J-3 and J-6, are responsible for operational and technical oversight for GCCS and report to the GCCS General Officer/Flag Officer Advisory Board. The Joint Staff, J-3 and J-6, relationships are depicted in Figure A-1 and defined in the following subparagraphs.

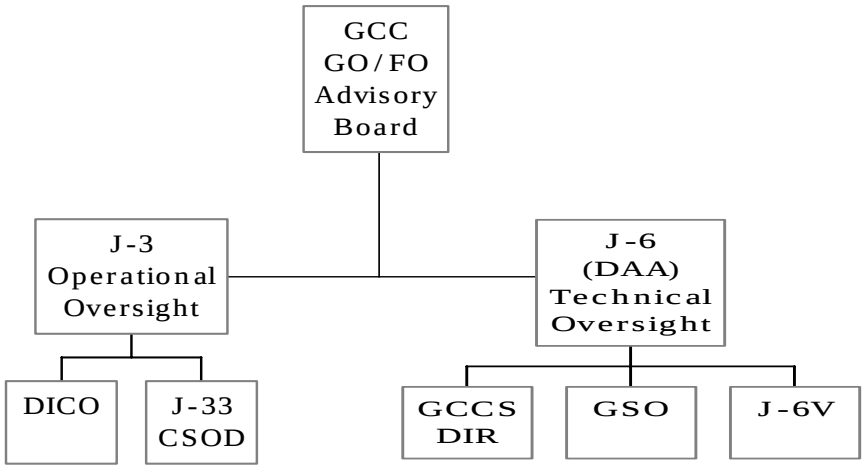


Figure A-1. JOINT STAFF GCCS OVERSIGHT ORGANIZATIONS

a. Director for Operations, Joint Staff (J-3). As directed in reference a, the Joint Staff, J-3, is the office of primary responsibility (OPR) for GCC and operational oversight of the GCCS. Proposed GCCS changes that will require a new evolutionary build or a new baseline will be reviewed and approved/disapproved by the J-3 at the GCC General/Flag Officer Advisory Board. A planner level GCCS Review Board, the C4 Systems Integration Working Group (C4SIWG), and functional area working groups assist the OPR.

(1) Data Information Coordination Office (DICO). The Joint Staff, J-3, will designate a DICO to provide operational direction and guidance for the GCCS. The J-3 DICO will be the primary focal point for any issue that may impact operations of the GCCS. The J-3 DICO shall have the authority to authorize extended system outages, priority of repairs, and other activities deemed critical to operation of the GCCS.

(2) Joint Staff J-33/Command Systems Operation Division (CSOD)). The Joint Staff J-33/CSOD is the OPR for management oversight of new functional requirements and proposals for migration of systems to GCCS, as specified in reference b. The J-33/CSOD provides the focal point for ensuring a responsive front-end process exists to identify, validate, integrate, and prioritize functional requirements.

b. Director for Command, Control, Communications, and Computer Systems (C4), Joint Staff (J-6). The Joint Staff, J-6, has technical oversight of GCCS. The J-6 will work closely with the J-3 and DISA to ensure smooth execution of this policy. Additionally, the J-6 is the GCCS Designated Approving Authority (DAA) for all GCCS security matters. The DAA is responsible for approving security policies, providing security guidance, and taking whatever actions are necessary to ensure the integrity and security of GCCS operations. Duties and responsibilities for the GCCS DAA are outlined in reference c.

(1) GCCS Director (DIR). The J-6 will designate a planner-level (O-6) GCCS DIR to be the focal point for all aspects of GCCS operations related to system and network configuration, fault, performance, and security management. The GCCS DIR is responsible for testing, evaluating, and implementing the GCCS. Additionally, the GCCS DIR will coordinate with OPRs of complementary systems, such as the Global Combat Support System (GCSS), in order to facilitate integration and merger, as required. The GCCS DIR will provide technical solutions or recommend changes to the DICO on global GCCS problems.

(2) GCCS Security Officer (GSO). The J-6 will designate a GSO. The GSO is responsible for day-to-day security operations of the GCCS. The GSO is responsible for providing security information and recommendations to the Joint Staff, DAA. for matters involving the GCCS. Responsibilities and duties for the GSO are outlined in references c and d.

(3) Joint Staff (J-6V). The J-6V is responsible for CM technical oversight. J-6V will co-chair the GCCS Configuration Management Board (CMB). J-6V and J-33/CSOD will review and approve outages to apply modifications to the GCCS operational environment, as required.

The J6V is responsible for ensuring the GCCS Program Office complies with requirement, cost, and schedule baseline control during system implementation and reports any baseline deviations. Additionally, J6V will ensure that baseline deviations are reported to the GCC Management Structure.

2. DISA. The Director of DISA is responsible for all configuration control (CC) activities outlined in this instruction, and network management and other processes that directly impact GCCS configuration. DISA also has responsibility for coordination with OPRs for systems, such as GCSS, to facilitate integration and merger, as required. The DISA organizations responsible for CC are depicted in Figure A-2 and collectively perform the following tasks.

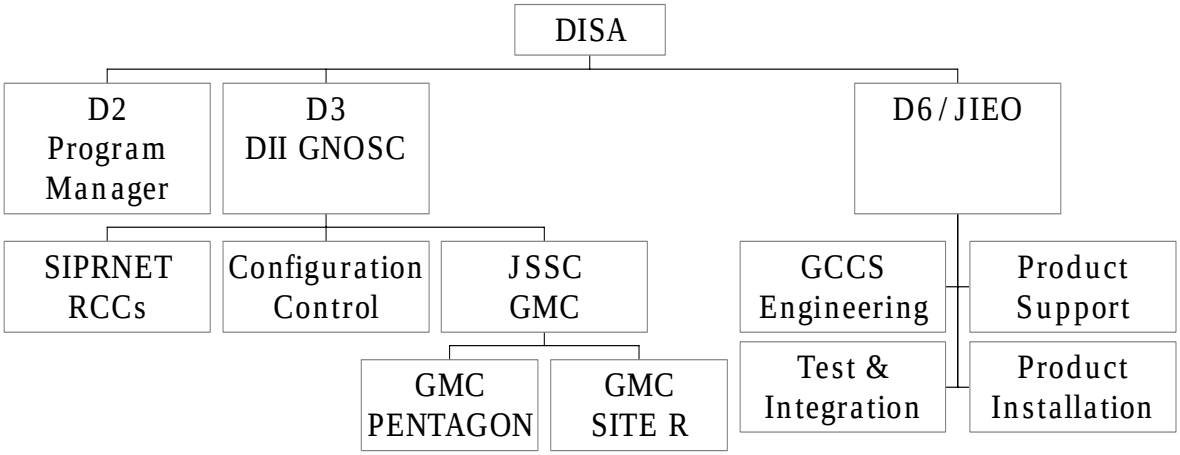


Figure A-2. DISA GCCS ORGANIZATIONAL RELATIONSHIPS

a. Co-chair the GCCS Configuration Management Board (CMB).

b. Coordinate and integrate activities of all DISA organizations working GCCS CC issues.

c. Coordinate with C/S/As to receive, test, and evaluate proposed mission unique or site unique configuration items (CIs) that may impact the GCCS operational environment. Following technical evaluation, provide J3 with a recommendation to approve or disapprove installation. Coordination will occur prior to any mission unique or site unique CIs being installed.

d. Integrate C/S/A CC efforts to optimize efficiency and eliminate redundant and/or contradictory efforts.

e. Monitor GCCS sites to ensure baseline configurations are maintained and pertinent functional, performance, and physical interfaces between GCCS components and software segments are adequately documented.

f. Coordinate efforts of individual GCCS configuration control boards (CCB) as outlined in Enclosure B, to define GCCS CIs required to be baselined and determine the documentation that must support all CIs. C/S/A GCCS sites will cooperate in this effort to ensure adherence.

g. Ensure that GCCS CIs are placed under configuration control when the CI is identified.

h. Ensure that change requests or evolutionary builds are processed and evaluated in a timely manner.

i. Ensure cost, schedule, and performance aspects of change requests, problem reports, and engineering change proposals are known at the time of their consideration by the CMB or respective CCBs.

j. Ensure that DISA maintained specifications, documentation, data, and related baseline information are adequate.

k. Ensure that adequate user, system, and other documentation is created, tested, and maintained for DISA-controlled CIs.

l. Review C/S/A documentation for sufficiency, accuracy, and currency. Report any C/S/A that fails to provide adequate documentation to the C4SIWG.

m. Lead and/or coordinate all CC audit processes for GCCS.

n. Ensure that GCCS data standardization efforts are timely and conform to applicable DOD standards.

o. Coordinate changes to system security resulting from configuration changes with applicable DAA(s) to ensure acceptability.

p. Oversee all segment releases to the GCCS baseline and control all automatic upgrades to segments in the baseline (including C/S/A supplied segments that contain automatic update capability).

3. GCCS Sites. A GCCS Site is defined as all locations where GCCS equipment is installed (e.g., workstations, servers, communications, and devices). GCCS positions are depicted in Figure A-3.

GCCS Site(s) DAA	GCCS Site(s) Coordinator * (GSC)	GCCS Site(s) ISSO *	GCCS System Administrator (GSA)	GCCS Network Administrator (GNA)	GCCS Database Administrator (GDBA)

* - Mandatory Position

Figure A-3. GCCS POSITIONS

a. GCCS Site(s) Coordinator (GSC). The GSC is responsible for coordinating all system and network support activities within the GCCS site(s). The individual filling this role will be the primary focal point for coordinating with the Service Help Desk (if applicable), the GMC Help Desk, and other GCCS organizations. One of the major duties of this position will be to direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site. The GSC is also responsible for coordinating with DISA and providing proposed mission unique and site unique CIs for testing and evaluation prior to installation. For large organizations, the site commander or DAA may want to appoint additional personnel in this function. They will be referred to as an Assistant GCCS Site(s) Coordinator (AGSC). Since the GSC is a mandatory position, this person should be able to perform the duties of the following positions (with the exception of the GCCS Site(s) ISSO) if manpower constraints prevent additional staffing. A GSC may coordinate the activities at more than one GCCS Site (i.e., more than one physical location).

b. GCCS Network Administrator (GNA). The GNA is responsible for the day-to-day operation of the GCCS local area network (LAN); the communications devices (premise router, communications server, and intelligent hubs); and related GCCS equipment. Duties include, but are not limited to:

(1) Operate and maintain the LAN and LAN system interfaces.

(2) Add and remove communications hardware and software.

(3) Maintain the AUTODIN/DMS (future) interface.

(4) Identify and be capable of installing each LAN component.

(5) Troubleshoot network and communications problems.

(6) Provide expertise in protocol services.

c. GCCS System Administrator (GSA). The GSA is responsible for a variety of duties with the major focus being on maintaining GCCS servers and workstations, providing local user support, and troubleshooting site problems associated with the GCCS applications. Duties include, but are not limited to:

(1) Direct activities during and following emergency conditions to minimize loss of GCCS mission capabilities.

(2) Administer access permission lists based on ISSO guidance.

(3) Maintain the Network Information Services permissions program.

(4) Add/remove hardware and software.

(5) Perform system startups, backups, and upgrades.

(6) Generate periodic system performance and utilization summaries.

(7) Backup data and audit files on a routine basis.

(8) Coordinate management of GCCS User IDs with the ISSO.

(9) Diagnose system problems and reporting to the GSC, the C/S/A Help Desk (if applicable), and the GMC Help Desk.

(10) Monitor system performance to ensure optimal performance.

(11) Reconfigure GCCS to regain processing capabilities for non-routine equipment malfunctions.

(12) Assist users in determining the cause of failures.

d. GCCS Database Administrator (GDBA). The GDBA is responsible for day-to-day operation of databases located at GCCS sites. This may include the primary database server running the Oracle Relational Database Management System (RDBMS), the Sybase RDBMS, or the

Automated Message Handling System (AMHS) server application using the Verity Topic RDBMS. Duties include, but are not limited to:

(1) Coordinating incremental/partial backups of the databases with the GSC and the GMC-Pentagon.

(2) Generating periodic summaries of database performance and utilization.

(3) Coordinating database modifications with other site personnel.

(4) Monitoring all database applications for proper performance.

(5) Managing disk/tape storage.

(6) Diagnosing database and database-to-application problems and resolving or reporting to the GSC.

e. GCCS Site(s) DAA. The GCCS Site(s) DAA is responsible for local security policies and guidance to ensure the integrity and security of the GCCS operations are maintained. Receives direction and guidance from the Joint Staff (J-6) GCCS DAA or his designated representative. The GCCS Site(s) DAA is responsible for accrediting GCCS at the site.

f. GCCS Site(s) Information Systems Security Officer (ISSO). The GCCS Site(s) ISSO is responsible for ensuring the integrity and security of the local GCCS system and network as well as providing security information to site GCCS DAAs. The duties of the GCCS Site ISSO are identified in reference d.

(INTENTIONALLY BLANK)

ENCLOSURE B

GCCS CM STRUCTURE

1. Global Command and Control (GCC) Management Structure. The GCC Management Structure is defined in reference a. Primary bodies and functions of the GCC Management Structure are as follows:

a. GCCS Review Board. The Vice Director of the Command, Control, Communications, and Computer Systems Directorate (VJ-6) chairs the GCCS Review Board. It is the primary body charged with consolidating and validating changes to the GCCS, in accordance with references a and b. It also reviews and approves charters for the Functional Area Working Groups and the C4SIWG. All new requirements that have been validated by the Joint Staff, J-3, will be given to the GCCS Review Board to prioritize. These prioritized requirements will then be prepared for the GCC General/Flag Officer Advisory Board for approval/disapproval. The GCCS Review Board, as specified in this instruction, will also review recommendations and resolve issues forwarded by the C4SIWG and the GCCS CMB. It will forward issues that cannot be resolved (i.e., funding issues, new baselines, unresolved issues from other boards) to the GCC General/Flag Officer Advisory Board.

b. C4 Systems Integration Working Group (C4SIWG). The J-6V chairs the C4SIWG. This group oversees CM for the various working groups. The C4SIWG coordinates with the GCCS CMB to verify the suitability of all recommended modifications to the GCCS operational environment prior to implementation. In coordination with the J-33/CSOD, the C4SIWG coordinates on recommended outages to apply upgrades. Issues the C4SIWG cannot resolve will be forwarded to the GCCS Review Board. The C4SIWG will coordinate with DISA on performance of technical and programmatic audits and reviews and will provide recommendations as necessary to the GCCS Review Board.

2. GCCS Collaborative CM Environment. CM is a management discipline that applies technical and administrative direction to the development, production, and support life cycle of a CI. This discipline is applicable to hardware, software, networking infrastructure, processed materials, services, and related technical documentation. CM is an integral part of life-cycle management. The main objective of CM is to ensure the integrity of a product by documenting and providing full visibility of the product's present configuration and the status of achievement of its functional and physical requirements. Because of the inherent nature of distributed processing and communications environments, CM becomes a difficult task

and generally requires the efforts of many organizations to accomplish. The GCCS operational environment is a distributed processing and communications environment. Because of the number of diverse organizations involved in GCCS CM, a collaborative CM environment is established to manage GCCS CM. This collaborative CM environment is depicted in Figure B-1 and responsible organizations are identified in the following subparagraphs.

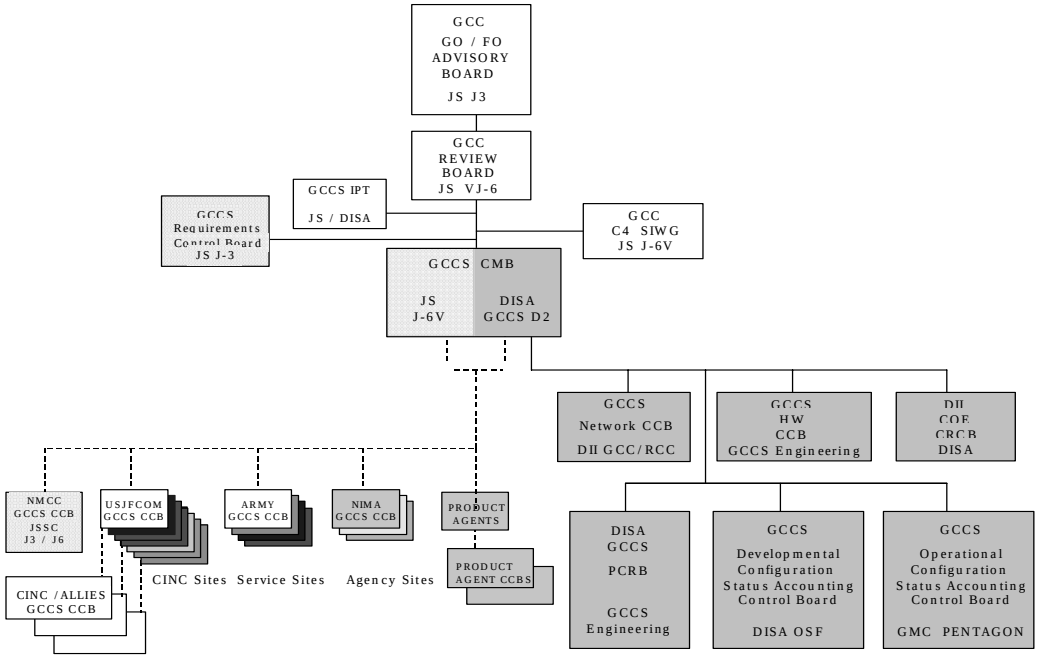


Figure B-1. GCCS COLLABORATIVE CM ENVIRONMENT

a. GCCS Configuration Management Board (CMB):

(1) Scope. The GCCS CMB is the primary authority for all GCCS product CM issues and oversees all other CM bodies. Its primary functions are to accept functional requirements from the Joint Staff, J3; designate configuration items (CI); control changes to CIs by ensuring that proposed changes satisfy functional requirements, CM requirements (such as configuration identification), and process requirements (such as quality and compliance testing); ensure other CM bodies and processes

are working properly by reviewing configuration status accounting and by initiating and reviewing configuration audits.

(2) Chair. The GCCS CMB will be co-chaired by the Joint Staff J-6V and DISA and is under the functional and technical oversight of the GCCS Review Board.

(3) Membership

(a) Regular Members. Regular CMB members are designated representatives from the Joint Staff (J6K, J6V, J33/CSOD) Executive/Product Agents, and DISA (D2, D6). Functional Area Working Group chairs, or their representatives will be invited to sessions with agendas applicable to that working group's area of responsibility. Others that may be included, as appropriate, are: Joint Staff (J-2, J-4, J-5, J-6, J-7, J-8), US Coast Guard, National Imagery and Mapping Agency, Defense Logistics Agency, National Security Agency, and OSD (C3I).

(b) Advisory Attendees. The co-chairs may invite advisory members.

(4) Meeting Frequency. The co-chairs will determine when to hold meetings. Announcement of meetings will be made as far in advance as possible to permit C/S/A representatives to attend.

(5) Charter. The requirements for a GCCS CMB charter are specified in Appendix A to this enclosure.

b. DII COE Configuration Review and Control Board (DCRCB):

(1) Scope. DISA shall establish a DCRCB to act as a forum for approval of proposed changes and improvements to common products and oversight of the software development process for the DII COE. The CRCB shall manage changes to common computer software configuration items (CSCI) used in subscriber systems. Common CSCIs include the common operating environment (COE), the associated engineering standards and conventions, and other software products selected by the CRCB for joint configuration management.

(2) Chair. DISA D6.

(3) Membership. As directed by the CRCB charter.

(4) Meeting Frequency. As directed by the chair.

(5) Charter. The DII COE CRCB is chartered in accordance with DISA guidance.

c. GCCS Hardware (HW) Configuration Control Board (CCB):

(1) Scope. The DISA D6 GCCS Engineering Office will be responsible for ensuring that hardware platforms implemented will adequately handle the processing and communications workload for each workstation. This requirement includes testing and evaluation of proposed additions to the joint software that is planned for each GCCS site. The GCCS HW CCB coordinates all hardware releases with the GCCS CMB.

(2) Chair. DISA D6.

(3) Membership. As directed by the chair. C/S/As may participate when issues pertain to them. DISA will place the upcoming agenda on SIPRNET so any C/S/A can determine if they should participate. DISA will provide adequate advance notice to permit CINC representatives to attend.

(4) Meeting Frequency. As directed by the chair.

(5) Charter. As directed by DISA.

d. GCCS Network CCB:

(1) Scope. The Global Control Center (GCC) that is operated by the DISA C4I Network Systems Management Division (D31) is the top level DII control center. The GCC provides management oversight for networks of the DII for which DISA has network management responsibility. These networks include the SIPRNET, the GCCS backbone communications infrastructure. The second level is comprised of the regional control centers (RCCs). The RCCs are responsible for day-to-day network operations under their immediate control. They are geographically oriented with several centers dispersed across the United States, a center located at the DISA European facility to cover Europe, and another located at the DISA Pacific facility to cover the Pacific assets. The RCCs are responsible for DISA assets within their areas and operate as peers to each other. The RCCs responsible for various portions of the SIPRNET are also responsible for the health of the DISN routers installed on those networks. The RCCs and the GCC are responsible for DISA assets only. They do not control any assets owned by individual C/S/As connected to

networks or WANs. The GCCS premise routers are included in the list of equipment that the GCC and the RCCs do not manage. The GCCS community is responsible for managing these assets. This is where the third level of the hierarchy model comes in to play. These management centers, or DII control centers, are referred to as local control centers (LCCs) and they belong to the individual subscriber communities. In the case of GCCS, the community must establish LCCs to manage local GCCS assets. DISN RCCs will coordinate with GMC-Pentagon on all efforts to detect, isolate, and correct problems associated with the GCCS. The GCCS Network CCB coordinates all Network CI releases with the GCCS CMB.

(2) Chair. DISA D3.

(3) Membership. As directed by the chair.

(4) Meeting Frequency. As directed by the chair.

(5) Charter. As directed by DISA.

e. GCCS Configuration Status Accounting (CSA) Control Board:

(1) Scope. DISA CM Division is responsible for the implementation of CIs and CSCIs, both prior to the operational implementation and throughout the life cycle of the CIs and CSCIs. All fielded GCCS CIs and CSCIs, including baselines and proposed changes, will be tracked by GMC-Pentagon. This board is comprised of a developmental section within DISA and an operational section within GMC Pentagon.

(2) Chair. DISA D6.

(3) Membership. As directed by DISA, but includes GMC-Pentagon and DISA CM Division.

(4) Meeting Frequency. As directed by DISA.

(5) Charter. As directed by DISA.

f. GCCS Site CCB (GSCCB):

(1) Scope. C/S/A GSCCBs may have an internal CM process, encompassing C/S/A specific configurables. This instruction does not address the CM process of individual C/S/As. The GCCS CMB will, however, control any C/S/A changes or configured items by enforcing

adherence to standards, if required. Issues not resolved by the GCCS CMB will be referred to the C4SIWG and GCCS Review Board. The GCCS Review Board will forward all issues it cannot resolve to the GCC General/Flag Officer Advisory Board. Those C/S/As with a GSCCB will comply with the following:

(a) GSCCBs shall notify GCCS GMC of proposed mission unique and site unique CIs prior to installation.

(b) GSCCBs shall ensure impacts of site-initiated modifications to GCCS are acceptable to affected parties.

(c) GSCCBs are responsible for site hardware/software configurations, inventories, and site unique applications residing on GCCS. The GSCCB will document and monitor site configuration and report all relevant configuration changes to GMC-Pentagon.

(d) GSCCBs will have a process to monitor and audit its GCCS hardware (this includes the hardware description, connections, locations, types, installation diagrams, clients/servers, etc.) and software (descriptions, versions, and documentation for applications and databases).

(2) Chair. As directed by the C/S/As.

(3) Membership. As directed by the C/S/As.

(4) Meeting Frequency. As directed by the C/S/As.

(5) Charter. As directed by the C/S/As.

g. GCCS Problem/Change Review Board (PCRB)

(1) Scope. The main task of the GCCS PCRB is evaluation of problem reports (PRs), change requests (CRs), and implementation of corrective action and/or modifications. GCCS Functional Working Groups will assist the GCCS PCRB with PR/CR priority establishment as defined in Enclosure D, subparagraph 2b and paragraph 3 of this instruction. The GCCS PCRB will provide user feedback to the C/S/As and Joint Staff concerning the priority of PRs/CRs. DISA will maintain, on line, the current status of all open GCCS PRs/CRs as they progress within the change management process. Any unresolved issues, or issues which extend beyond problem fixes, will be forwarded to the GCCS CMB for resolution. If a PR or CR is determined to be a new requirement

to the baseline reporting site will be notified and it will be forwarded through the GCCS CMB to the Joint Staff (J-33/CSOD) for processing.

(2) Co-chair. DISA D6 and GCCS Director.

(3) Membership. The PCRB will consist of members from the Joint Staff (J-3 and J-6), DISA D2/D6, GMC, and others designated by DISA or the GCCS Director. C/S/As may participate when issues pertain to them. DISA will place the upcoming PCRB agenda on SIPRNET so any C/S/A can determine if they should participate. DISA will provide adequate advance notice to permit C/S/A representatives to attend.

(4) Meeting Frequency. As directed by DISA and GCCS Director.

(5) Charter. GCCS PCRB charter requirements are specified in Appendix A to this enclosure.

(INTENTIONALLY BLANK)

APPENDIX TO ENCLOSURE B

CMB/CCB/PCRB CHARTERS AND MINUTES

1. Charters. The GCCS Review Board will approve charters for the GCCS CMB, CCBs and PCRB, as required. Each charter will contain the following:

a. Purpose and major objectives of the board.

b. Identification and responsibilities of the chair.

c. Membership responsibilities.

d. Advisory membership and responsibilities if applicable.

e. Relationships and responsibilities of the board to external organizations, to the GCC management structure, and to other boards with CM responsibilities.

f. Frequency of meetings, procedures for timely notification of attendees (including CINC representatives), and distribution list for minutes.

g. Procedures for modifying the charter.

2. Minutes and Dissemination of Information. A recorder will create the agenda, track action items, and record, publish and distribute minutes for each CMB/CCB/PCRB. Minutes will be available on line via SIPRNET. The DISA PCRB will provide monthly summaries to the GCCS CMB.

(INTENTIONALLY BLANK)

ENCLOSURE C

GCCS CM ACTIVITIES

1. Configuration Identification

a. Overview. Configuration identification includes selection of configuration items (CIs), determination of the types of configuration documentation required for each, the issue of numbers or identifiers affixed to each CI and the technical documentation describing its configuration (to include internal and external interfaces), the release of associated documentation, and the establishment of configuration baselines. All GCCS CIs will be controlled following the guidelines in references f, g, and h.

b. Designation of CIs. Items to be designated as CIs include:

(1) Any aggregation of hardware, software, materials, or any of their discrete portions that satisfy functional requirements and are useful to track for management purposes.

(2) Documents that describe technical aspects of the CIs such as functional specifications, design specifications, application programming interfaces (APIs), and operational specifications.

(3) Documents that describe CI management, configuration management and quality assurance processes, test plans, test reports, applicable minutes of CCBs, and user manuals.

c. Tasks. The purpose of configuration identification is to incrementally establish and maintain a definitive basis for configuration control and status accounting for a CI throughout its life cycle. To accomplish this DISA, C/S/A's, GSCs, and the Joint Staff will:

(1) Develop configuration documentation to define the configuration baselines for each CI, its components, and its interfaces.

(2) Establish a release system for configuration documentation.

(3) Align system requirements with CIs.

(4) Define and establish a quality assurance process (to include standards) for testing, documentation, product release, and providing CI information to Configuration Status Accounting personnel.

d. GCCS Software Applications Relationships. Understanding GCCS software application relationships provides the GCCS CM community with a logical method of controlling changes for the GCCS operational environment. DII COE Taxonomy is depicted in Figure C-1.

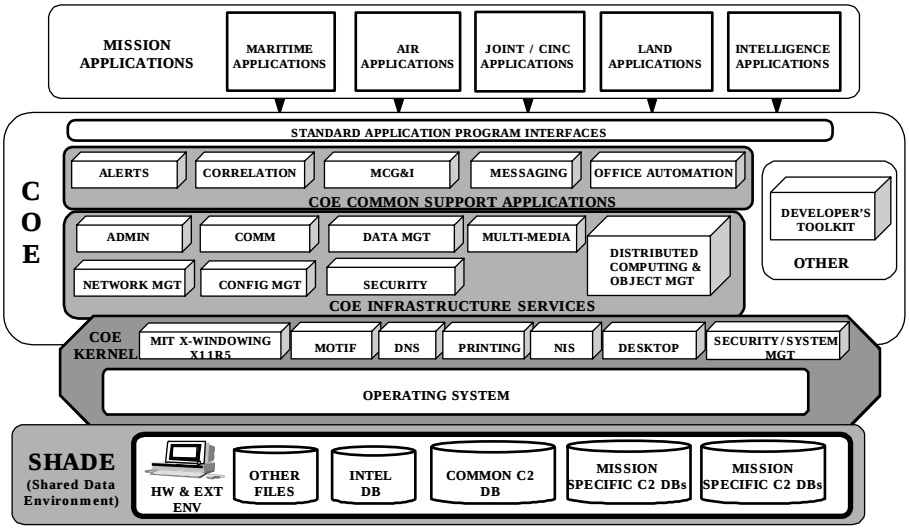


Figure C-1. DII COE TAXONOMY

The DII COE software illustrates the relationships between the Kernel, Infrastructure Services, and Common Support Applications. Figure C-1 also illustrates a conceptual view of how mission applications, interface with the DII COE through Application Program Interfaces (APIs). APIs provide joint mission applications, C/S/A mission unique applications, and site unique applications access to COE components. The COE and joint mission applications represent joint requirements. GCCS SW application examples are depicted in Figure C-2.

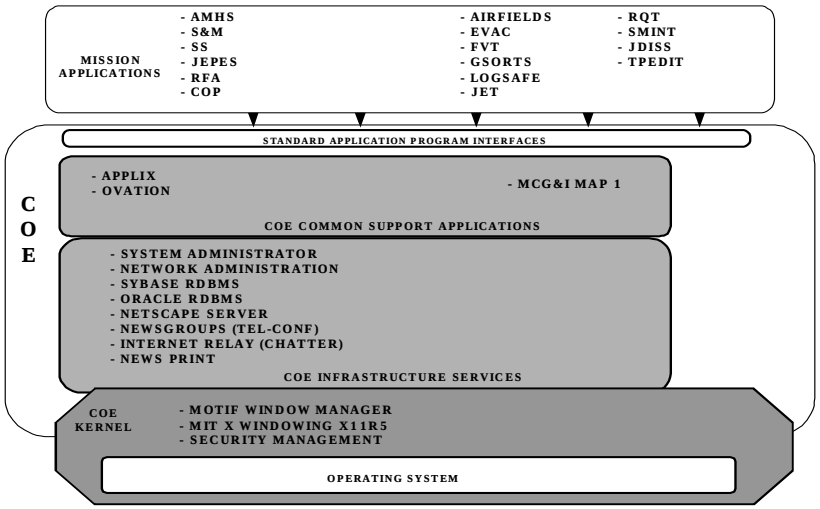


Figure C-2. GCCS SW APPLICATION EXAMPLES

The impacts of C/S/A mission unique and site unique applications must be acceptable to affected parties. They may reside in GCCS, but are not part of the joint mission requirements of GCCS. CIs in the COE are under control of the DII COE CRCB, and are subject to coordination with and approval by the GCCS CMB, C4SIWG, and Review Board for issues involving CIs comprising embedded user functionality. CIs for mission unique and site unique applications shall normally be under control of GCCS site CCBs and GSCs. However, GCCS CMB or PCRB may assume control, as required in the event of adverse system impact.

2. Configuration Control. Configuration control is the systematic proposal, justification, evaluation, coordination, and approval/ disapproval of proposed changes, and the implementation of all approved changes. The goals of configuration control are to:

a. Ensure effective control and oversight of all CIs and their approved configuration documentation.

b. Ensure regulated flow of proposed changes, documentation of the impact of proposed changes, and release of only those changes that have been approved.

c. Ensure that impacts of changes, to include C/S/A mission unique and site unique changes, are acceptable to affected parties.

d. Ensure changes are cost effective, timely, and meet users' needs.

e. Provide a change control forum where parties can discuss issues.

f. Manage engineering change proposal (ECP) and other change processes and oversee the implementation of approved changes.

g. Ensure proper implementation of all approved changes consistent with operational priorities.

h. Ensure integrated logistics support (ILS) is provided.

3. Configuration Status Accounting (CSA). CSA is the recording and reporting of information needed to manage CIs effectively. CSA occurs throughout the life cycle of the CI or the Computer Software Configuration Item (CSCI). The process begins with the initial registration of the CSCI by the segment developer or with the purchase of a hardware CI. Responsibility for CSA during this portion of the life cycle is primarily with DISA. Once the CI or CSCI becomes part of the operational system, through the shipment of a hardware CI to a GCCS Site or inclusion of a CSCI as part of an official release, CSA becomes primarily the responsibility of GMC-Pentagon.

4. Configuration Audits (CA). In the rapid prototyping environment, functional and physical configuration audits are not required. C/S/As who sponsor individual applications may conduct audits, as needed, prior to delivery of the application to DISA.

ENCLOSURE D

GCCS CM PROCESS

(Specific details of the GCCS CM process will be published in reference h.)

1. Engineering Change Proposals (ECP)/Change Requests (CR). ECPs, commonly referred to as CRs, will be submitted through the GSC, via the Service Help desk (if applicable), to the GMC Help Desk. The GMC Help Desk will record all ECPs for tracking and will forward them to the GCCS PCRB for formal action. The GCCS PCRB will evaluate the technical feasibility and provide cost estimates, technical recommendations, and scheduling implications to appropriate Functional Working Groups. These Functional Working Groups, serving as executive agents for the GCCS Review Board, will prioritize the ECPs and forward prioritized requirements via Joint Staff J-33/CSOD to the GCCS PCRB for appropriate action. Unresolved PCRB issues will be forwarded to the GCCS CMB and/or the GCCS Review Board for a decision.

a. Analysis of GCCS ECPs/CRs. DISA will monitor the full analysis of the ECP, to include costing and system impact.

(1) Mislabeled New Requirements. If analysis determines that an ECP is actually a new requirement, DISA will forward the ECP to the Joint Staff J-33/CSOD. DISA will inform the submitter that the ECP is a new requirement and has been forwarded to J-33/ CSOD and the submitter must follow the directions as outlined in reference b for new requirements. J-33 CSOD will log and track the new requirement in accordance with Enclosure D, paragraph 1 above.

(2) Mission Unique and Site Unique ECPs/CRs. C/S/As will indicate that an ECP or CR is for a mission unique or site unique CI. GSCs will inform GMC prior to installation. The impact of a proposed CI must be acceptable to affected parties. The determination of impact will include security aspects that may harm GCCS or the SIPRNET. GCCS connectivity must be analyzed to ensure a link is not vulnerable to intrusion attempts. If a CI is determined to impact GCCS or the DII COE, then the C/S/A will resolve the issue to DISA's satisfaction. C/S/As who do not agree with DISA findings may submit a waiver in accordance with paragraph 2 below. A memorandum of the problem and the resolution will be sent from the GCCS CMB to the C4SIWG prior to installation. This will be used for information purposes and will be forwarded to the GCCS Review Board.

b. Logging. All ECPs will be controlled and logged by DISA. The logged ECP will be updated to reflect the status of the ECP to include approved, applied, tested, documented, and integrated.

c. Approval. The implementation of ECPs will be approved by GCCS CMB with the exception of mission unique and site unique ECPs, which will be approved by the site GCS.

d. Closing ECPs. Closing an ECP requires written concurrence from the submitter or the GCCS CMB.

e. Classification of ECPs. Maintainers of the system in question will analyze the ECP, obtain user input, and classify it as either Class I (Emergency, Urgent, or Routine) or Class II. The classification of the ECP determines the priority order of analysis and implementation of the proposed change.

(1) Class I ECPs. Class I ECPs should be limited to those that offer significant benefit to the government. Normally, such changes correct serious deficiencies, add or modify interface or interoperability requirements, make significant and measurable effectiveness changes in operational environment capabilities or logistic supportability, or effect substantial life-cycle cost savings. An ECP could be a Class I if it would impact one of the following: safety; compatibility or specified interoperability with interfacing CIs or support software; configuration to the extent that retrofit would be required; operation or maintenance manuals for which adequate revision funding is not provided; interchangeability of CIs; sources of CIs or repairable items; skills, manning, training, or human engineering design.

(2) Types of Class I ECPs. The criticality of the need for a technical decision will dictate the priority of a Class I ECP. Target technical decision times are 48 hours for Emergency, 30 calendar days for Urgent, and 90 calendar days for Routine. C/S/As submitting ECPs will consider these targets when assigning a priority to the proposed change.

(a) Class I Emergency ECP (48 hours technical decision response time). An emergency priority will be assigned to a proposed Class I change for one of the following reasons:

1. To effect a change in operational characteristics which, if not completed without delay, may seriously compromise national security.

2. To correct a hazardous situation that may result in fatal or serious injury to personnel or may cause extensive damage or destruction of equipment.

3. To correct a significant system abnormal termination.

(b) Class I Urgent ECP (30 calendar day technical decision response time). An urgent priority will be assigned to a proposed Class I change for one of the following reasons:

1. To effect a change which, if not completed expeditiously, may seriously compromise mission effectiveness of equipment, software, or forces.

2. To correct a potentially hazardous condition that could result in injury to personnel or damage to equipment.

3. To effect a significant net life cycle cost savings to the government, as defined in the contract, through value engineering or through other cost reduction efforts where expedited processing of the change will be a major factor in realizing lower costs.

4. To correct unusable output critical to mission accomplishment.

5. To correct critical CI files that are being degraded.

(c) Class I Routine ECP (90 calendar day technical decision response time). A routine priority will be assigned to a proposed Class I change when emergency or urgent is not applicable.

(3) Class II ECP. A change that impacts none of the Class I factors previously specified is classified a Class II change. Class II ECPs will be incorporated into the next major release not yet in development.

2. Waiver Requests. Waiver requests are requests to modify or deviate from a requirement or specification due to changes in management direction, scheduling, cost, or some other compelling factor. The GCCS CMB will classify waiver requests as critical, major, or minor. A critical waiver requests a departure from a critical requirement or consists of

acceptance of a CI that does not conform to safety requirements. A major waiver requests a departure from a requirement consisting of acceptance of a CI involving requirements of performance, reliability, interchangeability, survivability, maintainability of the CI or its repair parts, effective use or operation, weight, or appearance (when a factor). A minor waiver requests a departure from a requirement consisting of acceptance of a CI that does not involve any factors listed above for critical or major.

a. Submission. All waivers will be submitted through the GSCs to the GMC Help Desk (except waivers related to new requirements or proposed migration systems).

b. Processing of Requests. The GCCS CMB will review and act on waiver requests. They will forward critical and major waiver requests with recommendations within 15 calendar days of receipt. They will forward minor waiver requests within 30 calendar days. The status of the waivers and their response will be reported to the submitter via SIPRNET. If the submitter does not agree with the response, then they may refer the request to the GCCS Review Board.

3. Change Control

a. Security. All CCB change control processes must adhere to references c and d. All CCBs will include a security representative as an ad hoc member.

b. SIPRNET Operational Control. The DISA Global Control Center (no organizational relationship with GCCS) has operational control of the SIPRNET up to the premise internet protocol (IP) router at the GCCS site. As previously stated in Enclosure B, subparagraph 2f, the GCC provides management oversight for the networks of the DII for which DISA has network management responsibility. These networks include the SIPRNET, the backbone communications infrastructure for GCCS. The RCCs responsible for various portions of the SIPRNET are also responsible for the health of the DISN routers installed on those networks. The RCCs and the GCC are responsible for DISA assets only. They do not control any assets owned by individual C/S/As connected to the networks or WANs. The GCCS premise routers are included in the list of equipment that the GCC and the RCCs do not manage. It is the responsibility of the GCCS sites or support organizations to manage these assets. GCCS sites will establish LCCs to manage the GCCS assets. The DISN RCCs will coordinate with the GMC Pentagon on all efforts to detect, isolate, and correct problems associated with the GCCS. Current SIPRNET accreditation policies for site local area network service

remains in effect, with oversight from the DISA Security Accreditation Working Group.

c. Connections Between GCCS Sites and Other Systems. Connections between GCCS sites and other systems require applicable DAA approval. A MOU must be written which details the scope of intrusion/cross-connection between the systems as it pertains to reference n. The Joint Staff (J-3/J-6) may direct DISA to direct C/S/As to disconnect systems from GCCS interfaces that violate this policy. Any change in the configuration of a connected system requires a review of the connection approval by the DAA.

d. Software (SW) Change Control Levels

(1) Joint Mission Area Application Change Control. Joint mission area applications are considered those that support multiple C/S/As. The following comprise joint mission area applications change control:

(a) Documentation Required from C/S/A. C/S/As will provide all necessary documentation for life cycle support, to include GCCS specific user manuals. C/S/As will provide to the GCCS CMB, hard copy and electronic documentation in a standardized format defined by DISA.

(b) Funding for Documentation. Documentation for C/S/A provided functionality is the responsibility of the C/S/A in accordance with the provisions of a MOU. DISA and the C/S/A will negotiate the terms of funding for documentation during the MOU coordination process or during C/S/A major segment releases. Any unresolved issues will be forwarded to the GCCS CMB and/or the GCCS Review Board for resolution.

(c) Software Certification. C/S/As will certify that all software segments are compliant with the DII COE, security requirements have been met and segments are virus-free.

(d) Approval Authority for Changes. Subject to GCCS Review Board oversight, the GCCS CMB may deny the implementation of any change to joint mission area applications that negatively impacts the cost, schedule, and functionality of GCCS. DISA will maintain an archived copy of the baseline, while the C/S/A GCCS Site CCBs maintaining the CI will retain the original baseline of record.

(2) DII COE. The DII COE supports an open systems environment in accordance with the Department of Defense (DOD) Technical

Architecture Framework for Information Management (TAFIM) and the Joint Technical Architecture (JTA). The DII COE includes COTS and GOTS applications and standard APIs that run on multiple hardware platforms. The objective of the DII COE is to provide a common application environment that satisfies the individual needs of many DoD applications. This evolving environment will ensure successful integration of a common set of information processing services that supports individual mission area requirements. The DII COE CRCB will control modifications to the DII COE, with assistance from Joint Staff and the C/S/As.

(a) DII COE Application Categories. Individual DII COE applications belong to one of three general categories:

1. Kernel applications provide basic operating system services.

2. Infrastructure services supporting information flow throughout the DII network. These services are commonly found on a wide variety of commercially distributed systems and provide such capabilities as database managers and system administration.

3. Common support applications not directly supporting the flow of information throughout the network but are critical to interoperability. These services include end-user applications such as office automation products or mission oriented applications ("embedded user functionality") such as track correlators and alert services.

(b) Documentation Required. DII COE developers/maintainers will provide all necessary documentation for life cycle support.

(c) Software Certification. DISA shall certify that all software segments are compliant will DII COE requirements, security requirements have been met, and all segments are virus free.

(d) Approval Authority. The DII COE CRCB shall approve changes to the DII COE. If proposed changes to the DII COE include GCCS embedded user functionality, as defined in this policy, the GCCS CMB and the GCCS Review Board must also approve the changes and verify that the embedded mission application and/or functionality is not adversely impacted. DISA will maintain an archived copy of the baseline.

(3) C/S/A Mission Unique and Site Unique Requirements. If a C/S/A has requirements for mission unique or site unique functions

that are not joint requirements, they shall notify GMC before the installation of any CIs.

(a) DII COE Impact. Mission unique and site unique applications must demonstrate the capability to run on the DII COE without impacting other integrated products. Compliance with reference f is mandatory.

(b) Software Certification. C/S/As will certify that all software segments are compliant with the DII COE, security requirements have been met, and segments are virus free.

4. C/S/A developed mission applications may be proposed as candidates for inclusion in the GCCS baseline. Proposals should be made through applicable functional working group as defined in reference a. Minimum criteria for consideration of these proposals for entry to CM processing are:

a. Application satisfies a requirement outlined in the GCCS Requirements Database (GRiD).

b. Application is DII COE Level 7 compliant.

c. Application has an identified Executive/Product Agent who shall be responsible for application life-cycle maintenance.

d. Application has an identified subject matter expert.

e. Application has a documented program cost/schedule/performance baseline.

f. Data used by application must comply with DoD directives outlined in reference i.

g. Application has necessary documentation for life-cycle support. C/S/As will provide to the GCCS CMB, hard copy and electronic documentation in a standardized format defined by DISA. Minimum documentation requirements are:

(1) User's Manuals.

(2) System Administrator Manuals.

(3) Installation Procedures.

(4) Software Version Description.

(5) Interface Design/Control Document.

(6) Software Test Plan, Description, and Report.

(7) Training materials.

5. Product release criteria. Besides complying with entrance criteria outlined above, a product shall only be released after the CMB has evaluated the following areas and deemed a product ready for release.

a. Security.

b. GCCS system interoperability.

c. Functional user assessment (effectiveness and suitability).

d. Operational test.

6. Related Processes: Requirements and Problem Resolution.

a. New Functional Requirements. C/S/As and GCCS working groups may input requirements for GCCS. The C/S/A GCCS approving authority will input requirement using the GCCS Requirements Database (GRiD) as directed in reference b. The Joint Staff, J-33/CSOD, in coordination with the C4SIWG, will track and further disseminate requirements to Functional Area Working Groups for validation and recommendation as to the type of GCCS application that will satisfy the requirement (e.g., a joint mission area application or a DII COE segment). DISA is responsible for technical evaluation after completion of a functional validation.

(1) Functional Tracking. The Joint Staff J-33/CSOD and the Functional Area Working Groups will track the status of functional requirements in GRiD.

(2) Technical Tracking. DISA will maintain a database to track approved and implemented technical solutions that satisfy functional requirements. The Joint Staff, CINCs, Services, and other authorized users will have access to the database to determine status of these requirements.

b. Problem Reports (PR). A PR initiates the process of getting a malfunctioning CI fixed. PRs are coordinated through GCCS Site Coordinators (GSC). Every effort will be made to resolve the problem at

the GCCS Site. A GCCS Site unable to resolve a problem will forward a request for problem resolution to the Service Help Desk (if applicable). If the Service Help Desk cannot resolve the problem, the PR will be forwarded to the GMC Help Desk. Generally, Service Help Desks (if applicable) can resolve problems and prevent the GMC Help Desk from being flooded with problems that can be resolved at lower levels.

(1) If the GMC Help Desk cannot resolve a problem, it will forward the unresolved PR and its status to the Global Technical Assistance Center (GTAC). The GTACS will attempt resolution of the PR. If the PR can not be resolved quickly and easily, the PR becomes a GSPR and is turned over to the PCRB. The PCRB will evaluate the technical feasibility and provide cost estimates, technical recommendations, and scheduling implications to the appropriate Functional Working Groups. These Functional Working Groups, serving as executive agents for the GCCS Review Board, will prioritize the PRs and forward prioritized requirements via Joint Staff, J33/CSOD, to the GCCS PCRB for appropriate action. Unresolved PCRB issues will be forwarded to the GCCS CMB or GCCS Review Board for decision.

(2) All PRs will be recorded, even if solved immediately. All PRs submitted to the GCCS PCRB will be tracked in the CM system and made available to approved CM users via SIPRNET.

(3) GSCs are responsible for tracking and resolution of PRs for mission unique and site unique CIs.

(4) Joint Universal Lessons Learned (JULLS) are submissions of lessons learned from any source. They are usually a result of an exercise and generally identify problems that have occurred. GCCS related JULLS that are of a technical nature will be given to the GMC Help Desk and categorized as PRs. They will then be tracked by DISA as a PR.

(5) PRs that have been submitted may be converted to ECPs or new requirements proposals after they are reviewed by the GCCS PCRB. If converted, reporting site user will be notified of conversion and the PR status will be updated to reflect the change. PRs converted to ECPs or new requirements proposals will be tracked in the CM system under the new category.

(INTENTIONALLY BLANK)

ENCLOSURE E

REFERENCES

a. CJCSI 6721.01 Series, “Global Command and Control Management Structure”

b. CJCSM 6721.01, 30 March 1997, “Global Command and Control System (GCCS) Functional Requirements Evaluation Procedures”

c. CJCSI 6731.01 Series, “Global Command and Control Security Policy”

d. CJCSM 6731.01 Series, “Global Command and Control System (GCCS) Security Procedure Manual”

e. MIL-STD-973, "Military Standard [for] Configuration Management"

f. “Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS),” DISA Joint Interoperability Engineering Organization (JIEO), DISA

g. DOD Directive 5200.28, 21 March 1988, “Security Requirements for Automated Information Systems (AISs)”

h. CJCSM 6722.01 Series, “Global Command and Control System Configuration Management Policy” **(UNDER DEVELOPMENT)**

i. DOD Directive 8320.1-M, "Data Administration Procedures"

(INTENTIONALLY BLANK)

GLOSSARY

Part I - Abbreviations and Acronyms

ADP	automated data processing
ADPE	automated data processing equipment
AGSC	Assistant GCCS Site Coordinator
AMHS	Automated Message Handling System
API	application program interface
C4	command, control, communications, computers
C4I	command, control, communications, computers, and intelligence
C4IFTW	command, control, communications, computers, and intelligence for the warrior
CA	configuration audit
CCB	Configuration Control Board
CI	configuration item
CINC	commander in chief
CJCS	Chairman of the Joint Chiefs of Staff
CJTF	Commander, Joint Task Force
CM	configuration management
CMB	Configuration Management Board
COE	common operating environment
COTS	commercial-off-the-shelf
C/S/A	CINCs, Services, and Agencies
CSA	configuration status accounting
CSCI	computer software configuration item
CSOD	Command Systems Operations Division
DAA	designated approving authority
DBMS	Data Base Management System
DICO	Data Information Coordination Office
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
ECP	engineering change proposal
GCC	Global Control Center
GCCS	Global Command and Control System
GCCS DIR	GCCS Director

GDBA	GCCS Database Administrator
GMC	Global Command and Control System Management Center
GNA	GCCS Network Administrator
GOTS	government-off-the-shelf
GriD	GCCS Requirements Database
GSA	GCCS System Administrator
GSC	GCCS Site Coordinator
GSCCB	GCCS Site Configuration Control Board
GSO	GCCS Security Officer
HW	hardware
I&RTS	Integration and Runtime Specification
IOC	initial operational capability
IP	internet protocol
IS	information system
ISSO	Information Systems Security Officer
IT	information technology
JS (J3)	Joint Staff, Operations Directorate
JS (J6)	Joint Staff, Command, Control, Communications, and Computer Systems Directorate
JS	Joint Staff
JULLS	Joint Uniform Lessons Learned System
LAN	local area network
LCC	local control center
OPR	office of primary responsibility
OSD	Office of the Secretary of Defense
OSE	open systems environment
PCA	physical configuration audit
PR	problem report
PSA	Principle Staff Assistant
RCC	regional control center
RDBMS	Relational Database Management System
SHADE	shared data environment
SIPRNET	Secret Internet Protocol Router Network
SIWG	Systems Integration Working Group
SSA	Software Support Activity
SW	software

TAFIM	Technical Architecture Framework for Information Management
WAN	wide area network

Part II - Definitions

application program interface (API) - (1) The interface, or set of functions, between the application software and the application platform. [APP] (2) The means by which an application designer enters and retrieves information. [DII Master Plan, V5.0, NOV 1996] (3) A programmer's guide that describes the COE software libraries and services, and how to write software modules that interface with and use the COE services. (I&RTS, V2.0, OCT 95]

automated data processing (ADP) - Recording, filing, computing, and producing data by means of electronic computers and associated auxiliary equipment. [US Navy ADP Glossary]

Automated Information System (AIS) - Computer hardware, computer software, telecommunications, information technology, personnel, and other resources that collect, record, process, store, communicate, retrieve and display information. An AIS can include computer software only, computer hardware only, or a combination of the above. [DODD 8000.1]

Automated Message Handling System (AMHS) - The collection of interconnected user agents (UAs), message systems (MSs), and message transfer agents (MTAs) that convey messages from one user to another.

baseline - A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development and that can be changed only through formal chnage control procedures or a type of procedure such as configuration management. [IEEE STD 610.12]

C4I for the Warrior Vision - The realization of a global command, control, communications, computer, and intelligence system that directly links and supports the warriors -- combat troops of all Services -- who engage in military operations in a rapidly changing world, providing them with accurate and complete pictures of their battlespace, timely and detailed mission objectives, and the clearest view of their targets. [C4IFTW, J6] [DII Master Plan, V5.0, NOV 1996]

change requests - A generic term used to collectively refer to all types of requests that would result in changes in hardware, software/segments, documentation, or functionality. Possible types of change requests are engineering change proposals, new requirements, and proposals for migration systems.

client - A computer program, such as a mission application, that requires a service. Clients are consumers of data while servers are producers of data.

commercial-off-the-shelf (COTS) - Refers to an item of hardware or software that has been produced by a contractor and is available for general purchase. Such items are at the unit level or higher. Such items must have been sold and delivered to government or commercial customers, must have passed customer's acceptance testing, and must be operating under the customer's control and within the user environment. Further, such items must have meaningful reliability, maintainability, and logistics historical data. [TAFIM 2.0, vol. 1]

common operating environment (COE) - The COE is an integrated software infrastructure, which facilitates the migration and implementation of functional mission applications and integrated databases across information systems. The DII COE provides architecture principles, guidelines, and methodologies that assist in the development of mission application software by capitalizing on a thorough, cohesive set of infrastructure support services. The DII COE specification is derived from the complete TAFIM. [DII Master Plan, V5.0, NOV 1996]

configuration - Functional and physical characteristics of a product as defined in technical documents and achieved in the product. [ISO STD 10007:1995]

configuration audit - Examination to determine whether a configuration item conforms to its configuration documents. [ISO STD 10007:1995]

configuration baseline - Configuration of a product, formally established at a specific point in time, which serves as a reference for further activities. [ISO STD 10007:1995]

configuration control - Activities comprising the technical control of changes to a configuration item after formal establishment of the configuration documents. [ISO STD 10007:1995]

Configuration Control Board (CCB) - Group of technical experts with the assigned authority and responsibility to make decisions on system. [ISO STD 10007:1995]

configuration documents - Documents that define the requirements, design, build/production, and verification for a configuration item. [ISO STD 10007:1995]

configuration identification - Activities comprising determination of the product structure, selection of the configuration items, documenting the configuration item's physical and functional characteristics including interfaces and subsequent changes, and allocating identification characters or numbers to the configuration items and their documents. [ISO STD 10007:1995]

configuration item (CI) - Aggregation of hardware, software, processed materials, services or any of its discrete portions that is designated for configuration management and treated as a single entity in the configuration management process.

configuration management (CM) - [1] technical and organizational activities comprising: configuration identification; configuration control; configuration status accounting; and configuration auditing. [ISO 10007:1995]. [2] A discipline applying technical and administrative direction and oversight to: (a) identify and document the functional and physical characteristics of a configuration item, (b) control changes to those characteristics, and [c] record and report changes to processing and implementation status. [MIL-STD 973]

Configuration Management Board (CMB) - The name designated for the Joint Staff (J6V) and DISA (D2) jointly chaired board that manages all configuration aspects of the GCCS environment.

configuration status accounting (CSA) - (1) Formalized recording and reporting of the established configuration documents, the status of proposed changes and the status of the implementation of approved changes.

data - Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

database - Structured or organized collection of information, which may be accessed by the computer.

Database Management System - Computer application program that accesses or manipulates the database. [HCI Style Guide]

Defense Information Infrastructure (DII) - A seamless web of communications networks, computers, software, databases, applications, and other capabilities that meets the information processing and

transport needs of DOD users in peace and in all crises, conflict, humanitarian support, and wartime roles.

Defense Information System Network (DISN) - A sub-element of the DII, the DISN is the DOD's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner.

Data Information Coordination Office (DICO) - The Joint Staff Director for Operations (J-3) will designate a Data Information Coordination Office (DICO) to provide operational direction and guidance for the GCCS.

distributed database - (1) A database that is not stored in a central location but is dispersed over a network of interconnected computers. (2) A database under the overall control of a central database management system but whose storage devices are not all attached to the same processor. (3) A database that is physically located in two or more distinct locations.

distributed system - A system consisting of a group of connected, cooperating computers.

embedded user functionality - Embedded user functionality are those DII COE (non-COTS) applications/segments that provide mission functions required for users to do their jobs. These applications involve user issues, not just technical issues, that can significantly impact the way users do their jobs. Embedded user functionality is subject to more stringent oversight and controls by the GCCS CMB than are the COTS portions of the DII COE.

Engineering Change Proposal (ECP) - A proposed change to current approved GCCS joint mission area application configuration item(s) (CIs), and the documentation by which the change is described, justified, and submitted to the GCCS CMB and GCC Management Structure for approval or disapproval. An ECP is a request to change a CI specification or functional requirement, usually to enhance or supplement the functionality of the CI or system.

environment - In the context of the COE, all software that is running from the time the computer is rebooted to the time the system is ready to respond to operator queries after operator login. This software includes the operating system, security software, installation software, windowing

environment, COE services, etc. The environment is subdivided into a runtime environment and a software development environment.

evolutionary build - The practice of placing agreed-upon functional or technical requirements into a build package that will become a version baseline for a system.

function - Appropriate or assigned duties, responsibilities, missions, tasks, powers, or duties of an individual, office, or organization. A functional area is generally the responsibility of a PSA (e.g., personnel) and can be composed of one or more functional activities (e.g., recruiting), each consisting of one or more functional processes (e.g., interviews). [Joint Pub 1-02, DoDD 8000.1, and DoD 8020.1-M]

Global Command and Control System (GCCS) - A highly mobile, deployable command, control, communications, computers, and intelligence (C4I) system that supports forces for joint and combined operations throughout the spectrum of conflict anytime and anywhere in the world with compatible, interoperable, and integrated C4I systems.

GCCS Database Administrator (GDBA) - The GDBA is responsible for the day-to-day operations of the databases located at the GCCS site. This may include the primary database server.

GCCS Designated Approving Authority (DAA) - The Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6) is the designated approving authority (DAA) for all GCCS security matters. The GCCS DAA is responsible for approving security policies, providing security guidance, and taking whatever actions are necessary to ensure the integrity and security of the GCCS operations.

GCCS Director (GCCS DIR) - The Joint Staff Director for Command, Control, Communications, and Computers (J-6) will designate a GCCS Director (GCCS DIR). The GCCS DIR will be the focal point for all aspects of GCCS operations related to system and network configuration, fault, performance, and security management. This responsibility includes testing, evaluation, and implementation of the GCCS. The GCCS DIR will provide technical solutions to the DICO for an operational decision on global GCCS problems or recommended changes.

GCCS Management Center (GMC) - The GMC will be a collection of offices functioning under a single management umbrella. This collection will use a combination of COTS and GOTS system and network management applications to continually monitor the health of the GCCS. The GMC Pentagon will support the activities of all GCCS sites, the

GCCS Network Administrator (GNA) - The GNA is responsible for the day-to-day operation of the GCCS LAN, the data and applications servers, the communications devices (premise router, communications server, and intelligent hubs) and related GCCS equipment.

GCCS Security Officer (GSO) - The Joint Staff Director for Command, Control, Communications, and Computers (J-6) will designate a GCCS Security Officer (GSO). The GSO is responsible for day-to-day security operations of the GCCS. As such, all site GCCS Information System Security Officers (Site GCCS ISSOs) will be responsible to the GSO. The GSO is responsible for providing security information and recommendations to the Joint Staff DAA for matters involving the GCCS.

GCCS Site(s) Coordinator (GSC) - The GSC is responsible for coordinating all system and network support activities within the GCCS site. The individual filling this role will be the primary focal point for coordinating with the GMC and other GCCS organizations. One of the major duties of this position will be to direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site.

GCCS System Administrator (GSA) - The GSA is responsible for a variety of duties with the major focus on maintaining GCCS applications, providing local user support, and troubleshooting site problems associated with GCCS applications. This includes responsibility for determining if GCCS applications are properly storing correctly formatted data to the GCCS database servers.

GMC Help Desk - The GMC-Help Desk is the GCCS user's primary point of contact for all problems associated with the joint mission pertaining to hardware, software, network, or communications. The GMC-Help Desk will not be responsible for supporting C/S/A unique applications. Users should coordinate with their GCCS Site Coordinator/Service Help Desk to verify a problem really exists prior to contacting the GMC-Help Desk.

government-off-the-shelf (GOTS) - Software products developed by the government and distributed throughout the government for use.

hardware - (1) Physical equipment, as opposed to programs, procedures, rules, and associated documentation. (2) Contrast with software.

information - Any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information System (IS) - A system consisting of mission specific or functional applications, data, and technical architecture consisting of support applications, application platforms, and the external environment including devices such as terminals, printers, and communications networks.

information technology (IT) - The technology included in hardware and software used for Government information, regardless of the technology involved, whether computers, communications, micro-graphics, or others.

infrastructure - Infrastructure is used with different contextual meanings. Infrastructure most generally relates to and has a hardware orientation but note that it is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. Again note that just citing standards for designing an architecture or infrastructure does not include functional and mission area requirements for performance. Performance requirement metrics must be an inherent part of an overall infrastructure to provide performance interoperability and compatibility. It identifies the top-level design of communications, processing, and operating system software. It describes the performance characteristics needed to meet database and application requirements. It provides a geographic distribution of components to locations. The service provider for these capabilities defines the infrastructure architecture. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs. [DoD 8020.1-M]

initial operational capability (IOC) - (1) At the system level, IOC is the point at which some portion of the technical and operational specifications defined by the requirements documents have been achieved. The specific definition of IOC will vary for each system and would be negotiated between the PM, the user, and the O&M activity. (2) At the site level, IOC is the point at which the technical specifications of that portion of the system installed at a specific site meet the documented requirements, but some portion of testing and/or operational specifications remains to be accomplished. The specific definition of IOC is site specific and would be negotiated between the PM, the site manager, and the O&M activity.

interface - A connecting link or interrelationship between two systems, two devices, two applications, or the user and an application, device, or system.

Joint Universal Lessons Learned System (JULLS) - A formatted data base program which allow users to input, access and manipulate automated lessons learned. There are three types of JULLS records in the database: 1) Lessons Learned JULL - deals with a specific item noted during an exercise or operation; 2) Summary JULL - provides an overall picture of the objectives and results of an exercise or operation; 3) Assessment JULL - reports on the degree of success obtained from the testing of specific exercise objectives.

kernel COE - That subset of the COE component segments which is required on all workstations. As a minimum, this consists of the operating system, windowing software, security, segment installation software, and an Executive Manager.

Local Area Network (LAN) - A data network, located on a user's premises, within a limited geographic region. Communication within a local area network is not subject to external regulation; however, communication across the network boundary may be subject to some form of regulation.

mission area variant - A collection of segments which are relevant to a particular mission area (e.g., analysis, planning). A mission area variant is typically a list of workstation variants.

open system - A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: (1) to be ported with minimal changes across a wide range of systems, (2) to interoperate with other applications on local and remote systems, and (3) to interact with users in a style that facilitates user portability.

open systems environment (OSE) - The comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles.

platform - The entity of the Technical Reference Model that provides common processing and communication services that are provided by a combination of hardware and software and are required by users, mission area applications, and support applications.

physical configuration audit (PCA) - A formal examination of the

"as-built/produced" configuration of a configuration item to verify that it conforms to its product configuration documents.

portability - (1) The ease with which a system or component can be transferred from one hardware or software environment to another. [IEEE STD 610.12] (2) A quality metric that can be used to measure the relative effort to transport the software for use in another environment or to convert software for use in another operating environment, hardware configuration, or software system environment. [IEEE TUTOR] (3) The ease with which a system, component, data, or user can be transferred from one hardware or software environment to another. [TA]

Problem Report - A PR is a notification that a CI is not performing to its functional specification(s). A CI may be a segment, application, application module, interface, documentation, etc. PRs are also known as Global Command and Control System PRs or GSPRs.

Product Agent (formerly known as executive agent) - is responsible for developing and maintaining GCCS configurations items. They establish CM processes consistent with CM policies. They fund for operations, maintenance, and modification of applications for inclusion into the GCCS.

Relational Database Management System (RDBMS) - An automated system for managing databases whose structure tables have the following properties: (1) each row in the table is distinct from every other row; (2) each row contains only atomic data, that is, there is no repeating data or such structures as arrays; (3) each column in the relational table defines named data fields or attributes.

remote install - The ability to electronically install segments from a local site (such as the DISA Operational Support Facility) to a remote site (such as USACOM). In a "push" mode, the local site initiates and controls the segment installation. In a "pull" mode, the remote site initiates and controls the segment installation.

router - Generically, any machine responsible for making decisions on which path, out of several different paths, network traffic will follow.

runtime environment -The runtime context determined by the applicable account group, the COE, and the executing segments.

seamless interface - Ability of facilities to call one another or exchange data with one another in a direct manner. Integration of the user

interface that allows a user to access one facility through another without any noticeable change in user interface conventions.

segment - (1) A segment is a module of related software that performs a function or set of functions. (2) A collection of one or more Computer Software Configuration Items (CSCI) most conveniently managed as a unit. Segments are generally defined to keep related CSCIs together so that functionality may be easily included or excluded in a variant.

server type -A class of servers in a client/server architecture. Among the different types of servers are the following: Name, Directory, Authentication, Access Control, Cryptographic, Communications, Time, File, Data, Print, Mail, Electronic Data Interchange (EDI), Applications, Presentation, and Sensor Monitor/Actuator.

shared data environment (SHADE) - The SHADE is the standards-based architecture that supports one-time data entry through reusable Information Technology/data assets and standard data elements. SHADE consists of two components: (1) shared distributed databases of standard data structures and standard data. (2) infrastructure components which include shared data dictionary services, transformation software, interfaces, and data warehouses.

SIPRNET - The data communications component of the DISN used for SECRET data. SIPRNET uses the same Internet Protocol routing technology as in NIPRNET with additional security measures needed to protect classified data transmissions.

Site GCCS designated approving authority (Site GCCS DAA) - The Site GCCS DAA is responsible for local security policies and guidance to ensure the integrity and security of the GCCS operations are maintained. The Site GCCS DAA is responsible for accrediting GCCS at the site.

Site GCCS Information System Security Officer (Site GCCS ISSO) - The Site GCCS ISSO is responsible for ensuring the integrity and security of the local GCCS system and network. The Site GCCS ISSO is responsible for providing security information to the Site GCCS DAAs. The GMC will be supported by the Site GCCS ISSO appointed at these locations.

site variant - A collection of segments that are relevant to the mission needs of a specific site (e.g., CVN, TRANSCOM, CJTF). A site variant is typically a list of mission area variants.

Software Support Activity (SSA) - A DISA DII COE support organization which enters software segments into an online library for configuration

management and confirms DII compliance. The SSA then tests interaction between segments and the impact on performance, memory utilization, etc.

system software - Computer programs that control, monitor, or facilitate the use of an Automated Information System; for example, operating systems, programming languages, communications, input-output control, sorts, security packages, and other utility programs. Includes off-the-shelf application packages obtained from manufacturers and commercial vendors such as for word processing, spreadsheets, database management, graphics, and computer-aided design.

system variant - A collection of segments that are relevant to a specific defined mission area (e.g., C4I, logistics, finance). GCCS and GCSS are two examples of a system variant. A system variant is typically a list of site variants.

Technical Architecture Framework for Information Management (TAFIM)- The TAFIM is a set of documents produced by DISA for the OSD to guide DOD information systems toward an open systems architecture. It provides the services, standards, design concepts, components, and configurations that can be used to guide the development of technical architectures that meet specific mission requirements.

user - (1) Any person, organization, or functional unit that uses the services of an information processing system. (2) In a conceptual schema language, any person or any thing that may issue or receive commands and messages to or from the information system.

variant - A subset of the superset of all software. This subset includes the COE and is fielded to service an operational mission area. A variant represents that collection of segments, including COE component segments, suitable for a particular site, mission area, or workstation.